Rec'd PCT/PTO 03 AUG 2001

FORM-PTO-1390 (Rev. 12-29-99) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER: 018773-030

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U S APPLICATION NO. (If known, see 37 C.F R. 1.5): Unassigned 09/890800

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/JP00/00474	January 28, 2000	January 28, 2000

TITLE OF INVENTION: Communication Management Table Transfer System, Manager, Encryptor, and Communication Management...

APPLICANT(S) FOR DO/EO/US: Noriko TAKEDA, Akihiko SASAMOTO, Kazuyuki ADACHI and Seiichi SHINODA

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and the PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☐ Other items or information:

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	JC05 Rec'd PCT/PTO 03 AUG 2001	ATTORNEY'S DOCKET NUMBER
Unassigned 09/890800	PCT/JP00/00474		018773-030

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1,000.00 (960)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00 (970)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00 (958)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00 (956)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	12 -20 =	0	X$18.00 (966)	$ 0	
Independent Claims	4 -3 =	1	X$80.00 (964)	$ 80.00	
Multiple dependent claim(s) (if applicable)			+$270.00 (968)	$	
TOTAL OF ABOVE CALCULATIONS =				$ 940.00	
Reduction for 1/2 for filing by small entity, if applicable (see below).				$	-
SUBTOTAL =				$ 940.00	
Processing fee of **$130.00 (156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 940.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$ 980.00	
				Amount to be: refunded	$
				charged	$

a. ☐ Small entity status is hereby claimed.

b. ☒ A check in the amount of $ 980.00 to cover the above fees is enclosed.

c. ☐ Please charge my Deposit Account No. 02-4800 in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

d. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Platon N. Mandros
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

William C Rowland, RN 30888, for
SIGNATURE

Platon N. Mandros
NAME

22,124
REGISTRATION NUMBER

(01/01)

09/890800
JC05 Rec'd PCT/PTO 03 AUG 2001

Patent
Attorney's Docket No. 018773-030

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Noriko TAKEDA et al.	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: August 3, 2001	)	
	)	
For: Communication Management Table...	)	

JC05 Rec'd PCT/PTO 03 AUG 2001

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination of the above-captioned patent application, kindly enter the following amendment.

IN THE SPECIFICATION:

Kindly replace the paragraph beginning at page 2, line 1, with the following:

-- On transferring data via the Internet, IP security compliant system is used for preventing an attack from the outside. Here, IP security means security securing system at IP packet level, defined by the IETF (Internet Engineering Task Force) which is a standardization organization for the Internet communication rules. --

IN THE CLAIMS:

Kindly replace Claim 9 as follows.

9. The encryptor of claim 7, wherein the communication management table includes a public key, and

the encryptor further comprising:

a secret key for secret communication exchanger for sharing a secret key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side.

Kindly replace Claim 10 as follows.

10. The encryptor of claim 7, wherein the communication management table includes a public key, and

the encryptor further comprising:

an certification key for secret communication exchanger for sharing an certification key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side.

10509907 090660

REMARKS

By way of the foregoing amendments to the specification errors have been corrected to improve the form of the application. No new matter has been introduced.

Early and favorable consideration with respect to this application is respectfully requested.

These changes have been made in accordance with 37 C.F.R. § 1.121 as amended on November 7, 2000.

Should any questions arise in connection with this application, the undersigned respectfully requests that he be contacted at the number indicated below.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: William Charles Jen 30222, for
Platon N. Mandros
Registration No. 22,124

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: August 3, 2001

TRADEMARK 09806960

Attachment to Preliminary Amendment dated August 3, 2001

Marked-up Copy

Page 2, Paragraph Beginning at Line 1

On transferring data via the Internet, IP [securuty] security compliant system is used for preventing an attack from the outside. Here, IP [securuty] security means security securing system at IP packet level, defined by the IETF (Internet Engineering Task Force) which is a standardization organization for the Internet communication rules.

TOSHIBA "00960"

Attachment to Preliminary Amendment dated August 3, 2001

Marked-up Claims

9. The encryptor of claim 7, wherein the communication management table includes a public key, and

the encryptor further comprising:

a secret key for secret [key] communication exchanger for sharing a secret key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side.

Kindly replace Claim 10, and add new Claim 10, as follows.

10. The encryptor of claim 7, wherein the communication management table includes a public key, and

the encryptor further comprising:

an certification key for secret [key] communication exchanger for sharing an certification key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side.

09/890800
JC05 Rec'd PCT/PTO 0 3 AUG 2001

ENGLISH TRANSLATION FOR PCT/JP00/00474

SPECIFICATION

Communication Management Table Transfer System, Manager, Encryptor, and Communication Management Table Transfer Method

Technical Field

The present invention relates to a communication management table transfer system including plural encryptors mutually connected through the Internet and a manager managing communication management table used by the plural encryptors for communication, and further relates to improvement of the security and the performance of the communication.

Background Art

Recently, system employing Virtual Private Network (VPN) has become popular. The VPN is a network in which a public network such as the Internet is virtually utilized as a private network using security technique such as encryption of data or authentication of a user. The virtual private network system enables to connect plural organizations through the public network as if they use exclusive communication lines like their internal network.

Fig. 13 shows an example of the virtual private network system. A reference numeral 1 shows the Internet, 11, 21, and 31 are encryptors, 12, 22, and 32 are routers, 13, 23, and 33 are firewalls, 14, 24, and 34 are subnets (internal networks), 15, 25, and 35 show communication terminals, and 36 shows a manager. These elements are connected as shown in the figure.

TOE080 "080686860

On transferring data via the Internet, IP securuty compliant system is used for preventing an attack from the outside. Here, IP securuty means security securing system at IP packet level, defined by the IETF (Internet Engineering Task Force) which is a standardization organization for the Internet communication rules.

In the IP securuty system, data transfer is performed after relation so-called SA (Security Association) is established between the encryptors of each internal network. By doing this, secret communication becomes possible. However, to establish SA requires to share a public key among the encryptors as a premise.

Further, in order to transfer data to the communication terminal of the internal network, it is necessary to know information of configuration of each internal network.

Accordingly, a communication management table including the public key and the configuration information of the internal network is generated, and the communication management tables are exchanged between the encryptors before establishing SA. The manager 36 is provided for generating, updating, and distributing the communication management table.

Conventionally, upon request from the encryptor, the manager 36 distributes the communication management table to the encryptor unconditionally.

Fig. 14 shows a transfer process of the communication management table on turning electric power on according to the related art. When an encryptor A11 is powered on, the encryptor A11 sends an encryptor

initialization notice (S101). When the manager 36 receives the encryptor initialization notice (S101), the manager 36 sends a response to the encryptor initialization notice (S102). On receiving the response to the encryptor initialization notice (S102), the encryptor A11 issues a command to obtain the communication management table (S103) unconditionally, and the communication management table is thus transferred (S104).

Fig. 15 shows a transfer process of the communication management table on rebooting according to the related art. The manager 36 sends a reboot instruction (S201), and the encryptor A11 is rebooted after the encryptor A11 sends a response to the reboot instruction (S202). Hereinafter, the operation will be the same as one shown in Fig. 14.

In the above-described system, the number of transferring the communication management table is large, which decreases the performace of data transfer.

Further, there is another problem with respect to the security of the communication, that is, the number of chances may be increased that the communication management table is stolen by an improper user. Namely, the public key or the configuration information of the internal network may be stolen, and the secrecy of the data transfer between the encryptors cannot be secured.

The present invention is provided to eliminate the above conventional problems. The invention aims to reduce the number of transferring the communication management table, improve the performance of data transfer, reduce the chances of improper use of the communication management table, and thus the security of the

communication can be increased.

Disclosure of the Invention

According to the present invention, a communication management table transfer system includes:

plural encryptors connected to each other through Internet; and

a manager which manages the communication management table used for communication among the plural encryptors,

wherein each of the plural encryptors includes:

a communication management table memory of an encryptor side for storing a communication management table of the encryptor side which is the communication management table to be stored in the each of the plural encryptors;

a communication management table version memory of the encryptor side for storing a communication management table version of the encryptor side which is a version of the communication management table of the encryptor side; and

a communication management table version sender for sending the communication management table version of the encryptor side to the manager,

wherein the manager includes:

a communication management table memory of a manger side for storing a communication management table of the manager side which is the communication management table to be stored in the manager;

a communication management table version memory of the manager

TOSHIBA 00205860

side for storing a communication management table version of the manager side which is a version of the communication management table of the manager side;

a communication management table version receiver for receiving the communication management table version of the encryptor side from the encryptor;

a communication management table version checker for checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side; and

a communication management table sender for sending the communication management table of the manager side when the mismatch is found by the communication management table version checker,

wherein the encryptor further includes a communication management table receiver for receiving the communication management table of the manager side from the manager, and

wherein the communication management table memory of the encryptor side stores the communication management table of the manager side received by the communication management table receiver as the communication management table of the encryptor side.

The communication management table transfer system of the invention,

wherein the communication management table sender further sends the communication management table version of the manager side when the mismatch is found by the communication management table version checker,

TOSHIBA 00005960

wherein the communication management table receiver further receives the communication management table version of the manager side from the manager, and

wherein the communication management table version memory of the encryptor side stores the communication management table version of the manager side received by the communication management table receiver as the communication management table version of the encryptor side.

According to the present invention, a manager managing a communication management table used for communication among plural encryptors connected to each other through Internet includes:

a communication management table memory of a manger side for storing a communication management table of the manager side which is the communication management table to be stored in the manager;

a communication management table version memory of the manager side for storing a communication management table version of the manager side which is a version of the communication management table of the manager;

a communication management table version receiver for receiving a communication management table version of an encryptor side which is a version of the communication management table of the encryptor side to be store in the encryptor from each of the plural encryptors;

a communication management table version checker for checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side; and

EP 0 830 000 A2

a communication management table sender for sending the communication management table of the manager side when the mismatch is found by the communication management table version checker.

The manager of the invention, wherein the communication management table sender further sends the communication management table version of the manager side when the mismatch is found by the communication management table version checker.

The manager of the invention further includes a communication management table updater of the manager side for updating the communication management table of the manager side and the communication management table version of the manager side correspondingly.

The manager of the invention further includes a communication management table update information receiver for receiving communication management table update information which is information to be updated within the communication management table of the manager side.

According to the present invention, an encryptor connected to another encryptor through Internet and of which a communication management table used for communication is managed by a manager, the encryptor includes:

a communication management table memory of an encryptor side for storing a communication management table of the encryptor side which is the communication management table to be stored in the encryptor;

a communication management table version memory of the encryptor side for storing a communication management table version of the

JP2000-0060960

encryptor side which is a version of the communication management table of the encryptor side;

a communication management table version sender for sending the communication management table version of the encryptor side to the manager; and

a communication management table receiver for receiving a communication management table of a manager side which is the communication management table to be stored in the manager from the manager, and

wherein the communication management table memory of the encryptor side stores the communication management table of the manager side received by the communication management table receiver as the communication management table of the encryptor side.

The encryptor of the invnetion, wherein:

the communication management table receiver further receives a communication management table version of the manager side which is a version of the communication management table of the manager side from the manager; and

the communication management table version memory of the encryptor side stores the communication management table version of the manager side received by the communication management table receiver as the communication management table version of the encryptor side.

The encryptor of the invention, wherein the communication management table includes a public key, and

the encryptor further comprising:

TOE980006US

a secret key for secret key communication exchanger for sharing a secret key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side.

The encryptor of the invention, wherein the communication management table includes a public key, and

the encryptor further includes:

an certification key for secret key communication exchanger for sharing an certification key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side.

The encryptor of the invention, wherein:

the other encryptor is connected to a subnet; and

the communication management table includes subnet configuration information which is information related to a configuration of the subnet, and

the encryptor further includes:

an Internet communicating unit for communicating with the other encryptor through the Internet based on the subnet configuration information included in the communication management table of the encryptor side.

According to the present invention, a method for transferring a communication management table used for a communication management

TOSHIBA-0000960

table transfer system including:

plural encryptors connected to each other through Internet, each of which has a communication management table memory of an encryptor side for storing a communication management table of the encryptor side and a communication management table version memory for storing a communication management table version of the encryptor side; and

a manager managing the communication management table used for communication among the plural encryptors, which has a communication management table memory of a manager side for storing a communication management table of the manager side and a communication management table version memory for storing a communication management table version of the manager side,

the method includes:

sending the communication management table version of the encryptor side to the manager by the encryptor;

receiving the communication management table version of the encryptor side from the encryptor by the manager;

checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side by the manager;

sending the communication management table of the manager side by the manager when the mismatch is found by the checking and finding;

receiving the communication management table of the manager side from the manager by the encryptor; and

storing the communication management table of the manager side

TOSHIBA-0080960

received as the communication management table of the encryptor side by the encryptor.

Brief Explanation of the Drawings

Fig. 1 shows a configuration of an encryptor according to the present embodiment.

Fig. 2 shows a configuration of a manager according to the embodiment.

Fig. 3 shows a transfer procedure of the communication management table on turning electric power on according to the embodiment.

Fig. 4 shows a procedure for omitting the transfer of the communication management table on turning electric power on according to the embodiment.

Fig. 5 shows a transfer procedure of the communication management table on rebooting according to the embodiment.

Fig. 6 shows a procedure for omitting the transfer of the communication management table on rebooting according to the embodiment.

Fig. 7 shows a configuration of the communication management table according to the embodiment.

Fig. 8 shows a configuration of the communication management table according to the embodiment.

Fig. 9 shows a configuration of the communication management table according to the embodiment.

Fig. 10 shows data flow on establishing SA.

JP2000-0080860

Fig. 11 shows data flow on secret communication.

Fig. 12 shows a case in which subnet configuration information is used.

Fig. 13 shows a system in which virtual private network is employed.

Fig. 14 shows a transfer procedure of the communication management table on turning electric power on according to the related art.

Fig. 15 shows a transfer procedure of the communication management table on rebooting according to the related art.

JP2000-080660

Best Mode for Carrying out the Invention

Embodiment 1.

In the following, the present invention will be explained referring to the figures showing an embodiment.

Fig. 1 shows a configuration of an encryptor according the embodiment. A reference numeral 1001 shows a power controller, 1002 shows a reboot controller, 1003 shows an initializer, 1004 shows a communication management table memory of the encryptor side, 1005 shows a communication management table version memory of the encryptor side, 1006 shows a communication management table version encryptor, 1007 shows an initialization completion notifier, 1008 shows a communication management table download controller, and 1009 shows a communication management table receiver.

Fig. 2 shows a configuration of a manager according to the embodiment. A reference numeral 2001 shows a reboot instructor, 2002 shows an initialization completion receiver, 2003 shows a communication

management table version decryptor, 2004 shows a communication management table memory of the manager side, 2005 shows a communication management table version memory of the manager side, 2006 shows a communication management table version checker, 2007 shows a communication management table download instructor, and 2008 shows a communication management table sender.

Fig. 3 shows a procedure of transferring the communication management table on turning an electric power on according to the embodiment. Hereinafter, this procedure will be described referring to the configurations shown in Figs. 1 and 2.

At an encryptor A11 side, on turning electric power on, the power controller 1001 instructs initialization to the initializer 1003. When the initialization is completed, the initializer 1003 notifies the initialization completion notifier 1007 of completion of initialization. The initialization completion notifier 1007 sends an encryptor initialization completion notice (S301) to the initialization completion receiver 2002 of a manager 36. At this time, the encryptor initialization completion notice (S301) includes communication management table version encrypted by a public key of the manager 36.

The communication management table version is stored in the communication management table version memory 1005 of the encryptor side. The communication management table version stored in the communication management table version memory 1005 of the encryptor side is made correspondence to the communication management table of the communication management table memory 1004 of the encryptor side. In

EP 1 080 880 A1

this example, the communication management table version memory 1005 of the encryptor side is included in the communication management table memory 1004 of the encryptor side, however, the communication management table version memory 1005 can be separated from the communication management table memory 1004 of the encryptor side.

The communication management table version encryptor 1006 is configured to read the communication management table version from the communication management table version memory 1005 of the encryptor side, encrypt the communication management table version, and send the encrypted communication management table version to the initialization completion notifier 1007.

At the manager 36 side, the initialization completion receiver 2002 receives the encryptor initialization completion notice (S301), and the communication management table version decryptor 2003 decrypts the encrypted communication management table version. On the other hand, the communication management table checker 2006 reads the communication management table version stored at the manager 36 side from the communication management table version memory 2005 of the manager side. And then, the communication management table version checker 2006 compares these communication management table versions. Here, the communication management table version memory 2005 of the manager side is included in the communication management table memory 2004 of the manager side, however, they can be separated as long as the communication management table is made correspondence to the communication management table version.

TOSHIBA 00806350

As a result of comparison, when two communication management table versions mismatch, the communication management table version checker 2006 notifies the mismatch to the communication management table download instructor 2007.

On receiving the notice of the mismatch, the communication management table download instructor 2007 sends a communication management table download instruction (S302) to the communication management table download controller 1008 of the encryptor A11.

At the encryptor A11 side, on receiving the communication management table download instruction (S302), the communication management table download controller 1008 instructs the communication management table receiver 1009 to obtain the communication management table to receive the communication management table according to the procedure of file transfer.

On receiving the instruction to obtain the communication management table, the communication management table receiver 1009 sends a command to obtain the communication management table (S103) to the communication management table sender 2008 of the manager 36.

At the manager 36 side, on receiving the command to obtain the communication management table (S103), the communication management table sender 2008 reads the communication management table from the communication management table memory 2004 of the manager side, and transfers the file of the communication management table to the communication management table receiver 1009 of the encryptor A11 (S104).

At the encryptor A11 side, on finishing receiving the communication

TOSHIBA-0008660

management table, the communication management table receiver 1009 notifies the communication management table download controller 1008 of the completion of obtaining the communication management table. The communication management table download controller 1008 sends response to the communication management table download instruction (S105) to the communication management table download instructor 2007 of the manager 36. Further, the communication management table receiver 1009 stores the received communication management table in the communication management table memory 1004 of the encryptor side.

In the above example, the file of the communication management table including the communication management table version is transferred and stored in the communication management table memory 1004 of the encryptor side. However, the communication management table version can be separated from the communication management table. Namely, the file of the communication management table without the communication management table version and the file of the communication management table version can be transferred separately.

In this way, when the communication management table versions mismatch, the communication management table is transferred from the manager 36 to the encryptor A11. Further, the communication management table version is also transferred.

Fig. 4 shows a procedure of omitting the transfer of communication management table on turning an electric power on. Hereinafter, this procedure will be explained referring to the configuration shown in Figs. 1 and 2.

JP2003006960

The procedure up to the step where the communication management table version checker 2006 compares the communication management table versions is the same as described above.

As a result of comparison, when the communication management table versions match, the communication management table version checker 2006 notifies the match to the initialization completion receiver 2002.

The initialization completion receiver 2002 sends response to the encryptor initialization completion notice (S102) to the initialization completion notifier 1007. When the initialization completion notifier 1007 receives the encryptor initialization completion notice (S102), the procedure terminates. Namely, the communication management table is not transferred in case that the communication management table versions match.

The timing at which the encryptor A11 sends the communication management table version and the manager 36 checks the communication management table version is not limited to the timing of initialization. It can be another timing, for example, the timing of reboot, or a certain periodical timing.

Fig. 5 shows a procedure of transferring the communication management table on rebooting according to the embodiment. Further, Fig. 6 shows a procedure of omitting the transfer of the communication management table on rebooting according to the embodiment. The procedures are the same as ones shown in Figs. 3 and 4 except that the procedures start at rebooting based on a reboot instruction (S201) and a reboot instruction response (S202).

EP 2 080 360 A1

In the following, the configuration of the communication management table will be explained. Figs. 7, 8, and 9 show the configuration of the communication management table according to the present embodiment.

As well as a communication management table version 90, the communication management table includes Internet communication information such as Internet communication information A50, Internet communication information B60, and so on and subnet configuration information such as subnet configuration information A70, subnet configuration information B80, and so on.

The Internet communication information A50 is necessary for the encryptor A11 on communicating with another encryptor through the Internet 1. The Internet communication information B60 is also necessary for the encryptor B21 on communicating with another encryptor through the Internet 1.

Reference numerals 51, 61 show Internet addresses, 52, 62 show identifiers for the encryptors, 53, 63 show certificates, and 54, 64 show effective dates. The certificate includes the public key for SA.

The subnet configuration information A70 is information related to the configuration of a subnet 14. The figure shows information for one record, however, another record may be added when many communication terminals are included in the configuration of the subnet 14. This is the same as for the subnet configuration information B80.

Reference numerals 71, 81 show identifiers of the encryptors, 72, 82 show network addresses, and 73, 83 show net masks.

TOE090 "0980660

In case of an example shown in Fig. 7, the communication management table version 90 includes one version, corresponding to the updated status of the whole communication management table.

In case of an example shown in Fig. 8, the communication management table version 90 includes plural versions such as encryptor A information version 91, encryptor B information version 92, and so on. The encryptor A information version 91 corresponds to the updated status of the Internet communication information A50 and the subnet configuration information A70, and so on (including another subnet configuration information, if there exists any).

In case of an example shown in Fig. 9, the communication management table version 90 is subdivided and includes versions of encryptor A Internet communication information version 93, encryptor A subnet configuration information version 94, encryptor B Internet communication information version 95, encryptor B subnet configuration information version 96, and so on. The encryptor A Internet communication information version 93 corresponds to the updated status of the Internet communication information A50. The encryptor A subnet configuration information version 94 corresponds to the updated status of the subnet configuration information A70, and so on (including another subnet configuration information, if there exists any).

In cases of Figs. 8 and 9, it is possible to correspond the version to each information by storing a device identifier or an information identifier corresponding to each version.

The manager 36 includes a communication management table

update information receiver (not shown in the figure) receiving communication management table update information, which is information to be updated within the communication management table, and a communication management table updater of the manager side (not shown in the figure) updating the communication management table of the manager side and the communication management table version of the manager side correspondingly.

In case shown in Fig. 7, the communication management table update information receiver updates the communication management table version 90 on receiving the communication management table update information from any of the encryptors. In case shown in Fig. 8, the communication management table update information receiver updates either of or both of the Internet communication information A50 and the subnet configuration information A70, and further updates the information version 91 for the encryptor A. In case shown in Fig. 9, on receiving the communication management table update information from the encryptor A11, the communication management table update information receiver checks whether it is required to update either of or both of the communication management table update information related to the Internet communication information A50 and the communication management table update information related to the subnet configuration information A70 and updates the communication management table update information. Further, the communication management table update information receiver updates either of or both of the Internet communication information version 93 for the encryptor A and the subnet configuration

EP 2 080 360 A1

information version 94 for the encryptor A corresponding to the communication management table update information.

In case of subdividing the communication management table version as shown in Figs. 8 and 9, it is also effective that the communication management table version checker 2006 compares the communication management table version for each subdivided version, and only part of the mismatched version of the communication management table can be transferred by communication management table transfer (S104). In such a case, information indicating the transferred part is added to the communication management table download instruction (S302). The communication management table receiver 1009 updates only the indicated part of the communication management table memory 1004 of the encryptor side and also updates only the indicated part of the communication management table version memory 1005 of the encryptor side.

Next, an operation of establishing SA using the public key for SA included in the communication management table will be explained. Fig. 10 shows data flow on establishing SA. In this example, the encryptor A11 requests to establish SA, and the encryptor B21 responds to the request for establishing SA. Each encryptor has a secret key memory 1013 for SA storing a secret key for SA of its own encryptor and a certification key and secret key for secret communication exchanger 1010 for sharing a secret key 1011 for secret communication and a certification key 1012 for secret communication. The certification key and secret key for secret communication exchanger 1010 is configured so as to input the secret key for SA of its own encryptor and the public key for SA of the partner's encryptor.

1020*020860

The certification key and secret key for secret communication exchanger 1010 of the encryptor A11 generates a random number Xa, signatures, encrypts, and sends to the encryptor B21 (S501). The certification key and secret key for secret communication exchanger 1010 of the encryptor B21 generates a random number Xb. The certification key and secret key for secret communication exchanger 1010 of the encryptor B21 generates the secret key 1011 for secret communication and the certification key 1012 for secret communication by combining the random number Xb with the random number Xa. Further, the certification key and secret key for secret communication exchanger 1010 of the encryptor B21 signatures and encrypts hashed values of Xb and Xa, and sends them to the encryptor A11 (S502). The certification key and secret key for secret communication exchanger 1010 of the encryptor A11 generates the secret key 1011 for secret communication and the certification key 1012 for secret communication by combining the random numbers Xa and Xb, and checks the received hashed values. Further, the certification key and secret key for secret communication exchanger 1010 of the encryptor A11 sends the hashed value of the random number Xb to the encryptor B21 (S503). The certification key and secret key for secret communication exchanger 1010 of the encryptor B21 checks the received hashed value. Through the above procedure, SA is established. Consequently, both partners obtain the secret key 1011 for secret communication and the certification key 1012 for secret communication shared with each other.

In the following, an operation of the secret communication performed after establishing SA will be explained. Fig. 11 shows data flow of the secret

"0080960"

communication. In this example, the encryptor A11 sends data, and the encryptor B21 receives the data. The illustrated communication is only one of examples, since the communication can be bidirectional between the encryptors which have already established SA.

Each encryptor includes an Internet communication unit 1014 and a subnet communication unit 1015. The Internet communication unit 1014 controls the communication through the Internet 1, and the subnet communication unit 1015 controls the communication through the subnet.

In the Internet communication unit 1014 at the sender side, an encryption unit 1016, a certification unit 1017, and an encapsulation unit 1018 operate. In the Internet communication unit 1014 at the receiver side, a certification unit 1019, a decryption unit 1020, and a decapsulation unit 1021 operate. Within these operations, the secret key 1011 for secret communication is used for encryption algorithm, and the certification key 1012 for secret communication is used for authentication algorithm.

Further, the subnet configuration information included in the communication management table is used for communication to the subnet connected to another encryptor. As shown in Fig. 12, the subnet configuration information is used within the Internet communication unit 1014.

Industrial Applicability

According to the present invention, the communication management table version is managed between the manager and the encryptor. When the communication management tables are judged as identical between the

EP 0 880 960 A1

manager and the encryptor, the transfer of the communication management table is omitted. Therefore, the number of transferring the communication management table is reduced, which enormously improves performance and security of data communication.

TOSHIBA-0000360

Claims

1. A communication management table transfer system comprising:

plural encryptors connected to each other through Internet; and

a manager which manages the communication management table used for communication among the plural encryptors,

wherein each of the plural encryptors includes:

a communication management table memory of an encryptor side for storing a communication management table of the encryptor side which is the communication management table to be stored in the each of the plural encryptors;

a communication management table version memory of the encryptor side for storing a communication management table version of the encryptor side which is a version of the communication management table of the encryptor side; and

a communication management table version sender for sending the communication management table version of the encryptor side to the manager,

wherein the manager includes:

a communication management table memory of a manger side for storing a communication management table of the manager side which is the communication management table to be stored in the manager;

a communication management table version memory of the manager side for storing a communication management table version of the manager side which is a version of the communication management table of the manager side;

TE0880-00006850

a communication management table version receiver for receiving the communication management table version of the encryptor side from the encryptor;

a communication management table version checker for checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side; and

a communication management table sender for sending the communication management table of the manager side when the mismatch is found by the communication management table version checker,

wherein the encryptor further includes a communication management table receiver for receiving the communication management table of the manager side from the manager, and

wherein the communication management table memory of the encryptor side stores the communication management table of the manager side received by the communication management table receiver as the communication management table of the encryptor side.

2. The communication management table transfer system of claim 1,

wherein the communication management table sender further sends the communication management table version of the manager side when the mismatch is found by the communication management table version checker,

wherein the communication management table receiver further receives the communication management table version of the manager side from the manager, and

wherein the communication management table version memory of

0990800"0800301

the encryptor side stores the communication management table version of the manager side received by the communication management table receiver as the communication management table version of the encryptor side.

3. A manager managing a communication management table used for communication among plural encryptors connected to each other through Internet comprising:

a communication management table memory of a manger side for storing a communication management table of the manager side which is the communication management table to be stored in the manager;

a communication management table version memory of the manager side for storing a communication management table version of the manager side which is a version of the communication management table of the manager;

a communication management table version receiver for receiving a communication management table version of an encryptor side which is a version of the communication management table of the encryptor side to be store in the encryptor from each of the plural encryptors;

a communication management table version checker for checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side; and

a communication management table sender for sending the communication management table of the manager side when the mismatch is found by the communication management table version checker.

4. The manager of claim 3, wherein the communication management

TOSHIBA 00806860

table sender further sends the communication management table version of the manager side when the mismatch is found by the communication management table version checker.

5. The manager of claim 3 further comprising a communication management table updater of the manager side for updating the communication management table of the manager side and the communication management table version of the manager side correspondingly.

6. The manager of claim 5 further comprising a communication management table update information receiver for receiving communication management table update information which is information to be updated within the communication management table of the manager side.

7. An encryptor connected to another encryptor through Internet and of which a communication management table used for communication is managed by a manager, the encryptor comprising:

a communication management table memory of an encryptor side for storing a communication management table of the encryptor side which is the communication management table to be stored in the encryptor;

a communication management table version memory of the encryptor side for storing a communication management table version of the encryptor side which is a version of the communication management table of the encryptor side;

a communication management table version sender for sending the communication management table version of the encryptor side to the manager; and

EP 1 050 980 A2 000006860

a communication management table receiver for receiving a communication management table of a manager side which is the communication management table to be stored in the manager from the manager, and

wherein the communication management table memory of the encryptor side stores the communication management table of the manager side received by the communication management table receiver as the communication management table of the encryptor side.

8. The encryptor of claim 7, wherein:

the communication management table receiver further receives a communication management table version of the manager side which is a version of the communication management table of the manager side from the manager; and

the communication management table version memory of the encryptor side stores the communication management table version of the manager side received by the communication management table receiver as the communication management table version of the encryptor side.

9. The encryptor of claim 7, wherein the communication management table includes a public key, and

the encryptor further comprising:

a secret key for secret key communication exchanger for sharing a secret key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side.

KR 10-2008-0080960

10. The encryptor of claim 7, wherein the communication management table includes a public key, and

the encryptor further comprising:

an certification key for secret key communication exchanger for sharing an certification key for secret communication used for secret communication with the other encryptor through the Internet, with the other encryptor by using the public key included in the communication management table of the encryptor side.

11. The encryptor of claim 7, wherein:

the other encryptor is connected to a subnet; and

the communication management table includes subnet configuration information which is information related to a configuration of the subnet, and

the encryptor further comprising:

an Internet communicating unit for communicating with the other encryptor through the Internet based on the subnet configuration information included in the communication management table of the encryptor side.

12. A method for transferring a communication management table used for a communication management table transfer system including:

plural encryptors connected to each other through Internet, each of which has a communication management table memory of an encryptor side for storing a communication management table of the encryptor side and a communication management table version memory for storing a communication management table version of the encryptor side; and

TOSHIBA 00006660

a manager managing the communication management table used for communication among the plural encryptors, which has a communication management table memory of a manager side for storing a communication management table of the manager side and a communication management table version memory for storing a communication management table version of the manager side,

the method comprising:

sending the communication management table version of the encryptor side to the manager by the encryptor;

receiving the communication management table version of the encryptor side from the encryptor by the manager;

checking and finding mismatch of the communication management table version of the encryptor side received and the communication management table version of the manager side by the manager;

sending the communication management table of the manager side by the manager when the mismatch is found by the checking and finding;

receiving the communication management table of the manager side from the manager by the encryptor; and

storing the communication management table of the manager side received as the communication management table of the encryptor side by the encryptor.

TOSHIBA-0000960

Abstract

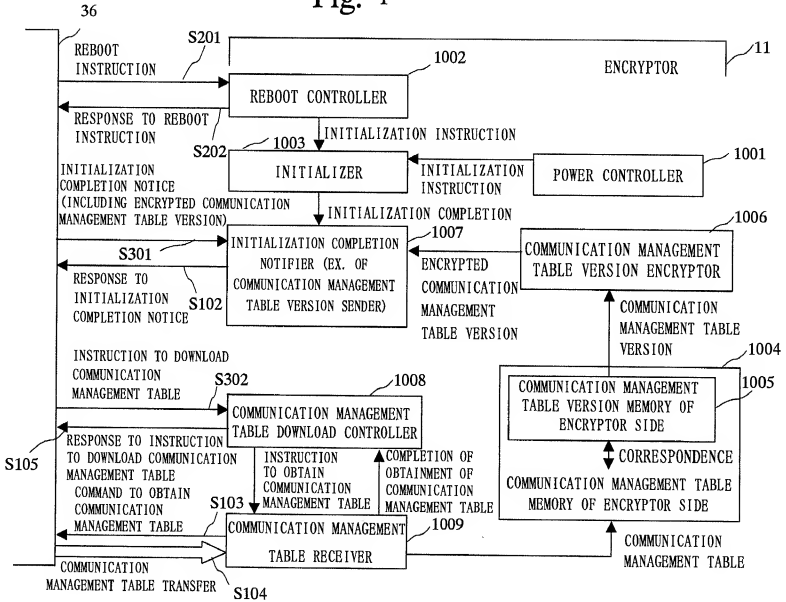
The present invention relates to a communication management table transfer system including plural encryptors mutually connected through the Internet and a manager which manages the communication management table used for the communication among the plural encryptors. The invention aims to improve security and performance of the communication.

On receiving a communication management table version from an encryptor 11 (S301), a manager 36 compares the received communication management table version with the communication management table version stored in a communication management table version memory 2005 of the manager side by using a communication management table checker 2006. The manager 36 transfers the communication management table to the encryptor 11 only when the mismatch is found (S104).

JP2003008606A

TOE080 00806860

Fig. 1



BURNS, DOANE, SWECKER AND MATHIS LLP
APPLN. FILING DATE: AUG. 3, 2001
TITLE: COMMUNICATION MANAGEMENT TABLE...
ATTORNEY DOCKET NO.: 018773-030
15 SHEETS
09/890800

Fig. 2

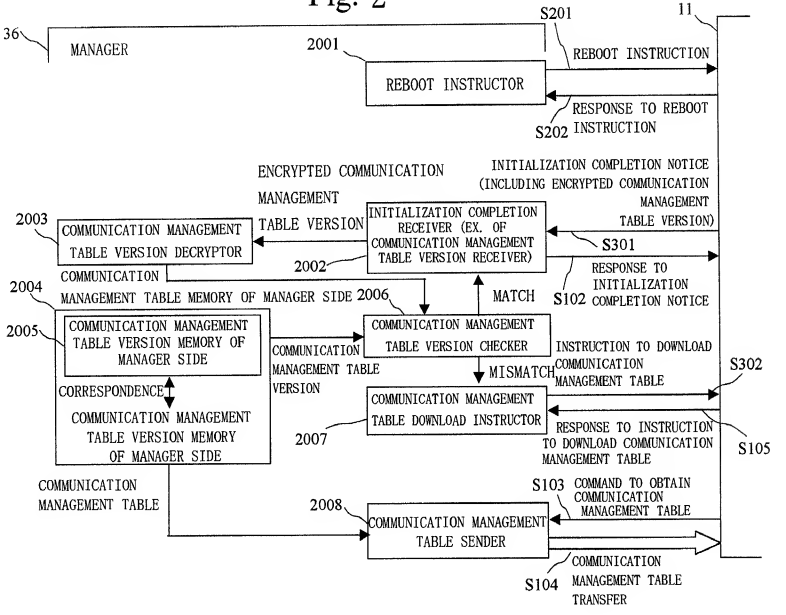
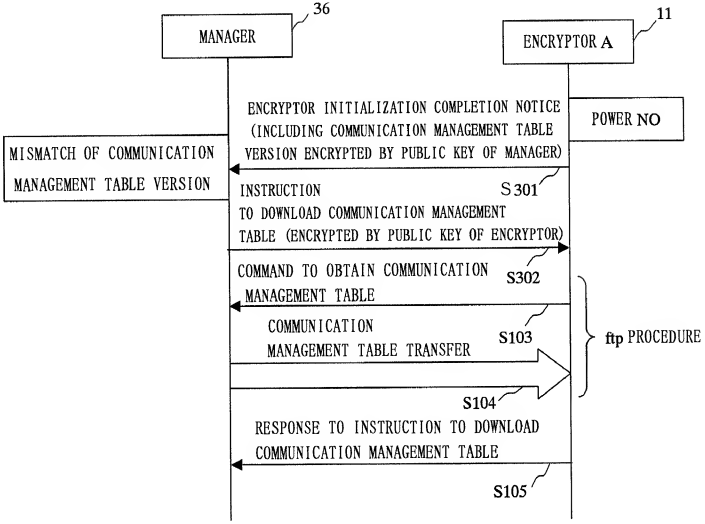
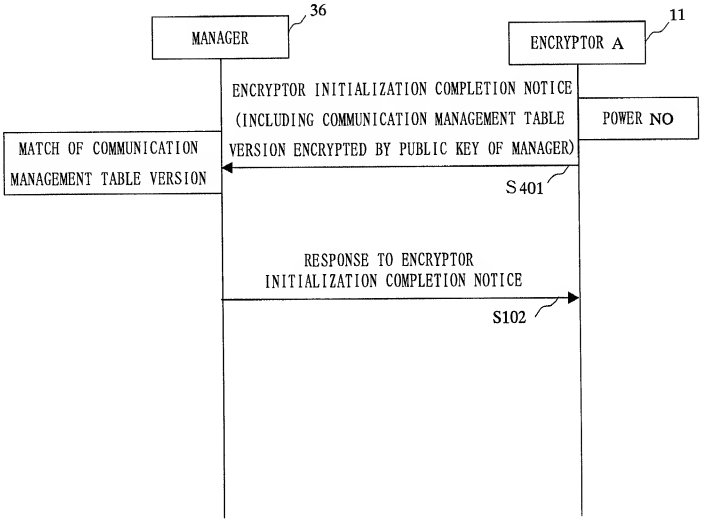

36
MANAGER
2001
REBOOT INSTRUCTOR
S201
11
REBOOT INSTRUCTION
RESPONSE TO REBOOT INSTRUCTION
S202
ENCRYPTED COMMUNICATION MANAGEMENT TABLE VERSION
INITIALIZATION COMPLETION NOTICE (INCLUDING ENCRYPTED COMMUNICATION MANAGEMENT TABLE VERSION)
2003
COMMUNICATION MANAGEMENT TABLE VERSION DECRYPTOR
INITIALIZATION COMPLETION RECEIVER (EX. OF COMMUNICATION MANAGEMENT TABLE VERSION RECEIVER)
S301
2002
COMMUNICATION MANAGEMENT TABLE MEMORY OF MANAGER SIDE
2004
2006
MATCH
RESPONSE TO INITIALIZATION COMPLETION NOTICE
S102
2005
COMMUNICATION MANAGEMENT TABLE VERSION MEMORY OF MANAGER SIDE
COMMUNICATION MANAGEMENT TABLE VERSION CHECKER
INSTRUCTION TO DOWNLOAD COMMUNICATION MANAGEMENT TABLE
S302
COMMUNICATION MANAGEMENT TABLE VERSION
MISMATCH
CORRESPONDENCE
COMMUNICATION MANAGEMENT TABLE VERSION MEMORY OF MANAGER SIDE
COMMUNICATION MANAGEMENT TABLE DOWNLOAD INSTRUCTOR
2007
RESPONSE TO INSTRUCTION TO DOWNLOAD COMMUNICATION MANAGEMENT TABLE
S105
COMMUNICATION MANAGEMENT TABLE
S103
COMMAND TO OBTAIN COMMUNICATION MANAGEMENT TABLE
2008
COMMUNICATION MANAGEMENT TABLE SENDER
S104
COMMUNICATION MANAGEMENT TABLE TRANSFER

Fig. 3



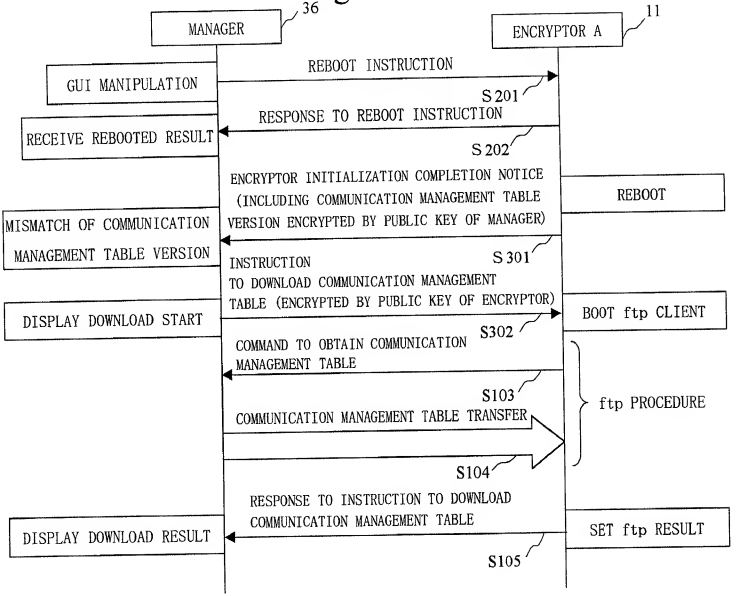
09/806860

Fig. 4



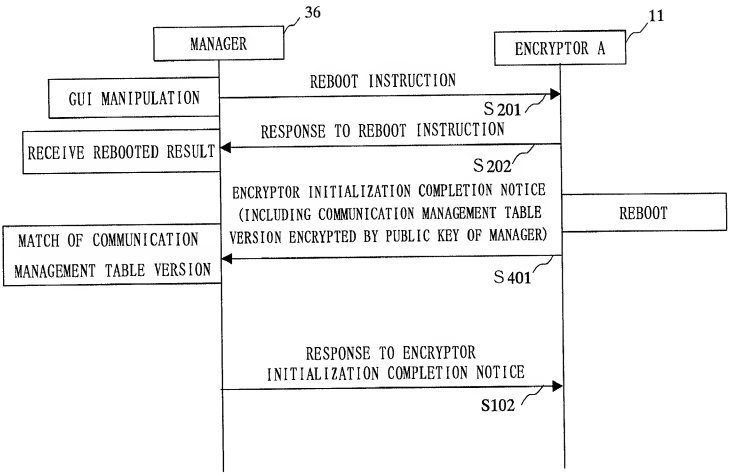
09/890800

Fig. 5



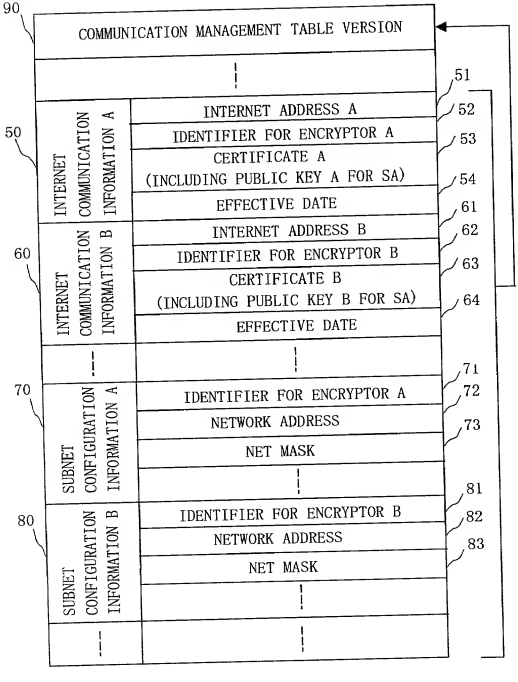
09/890000

Fig. 6



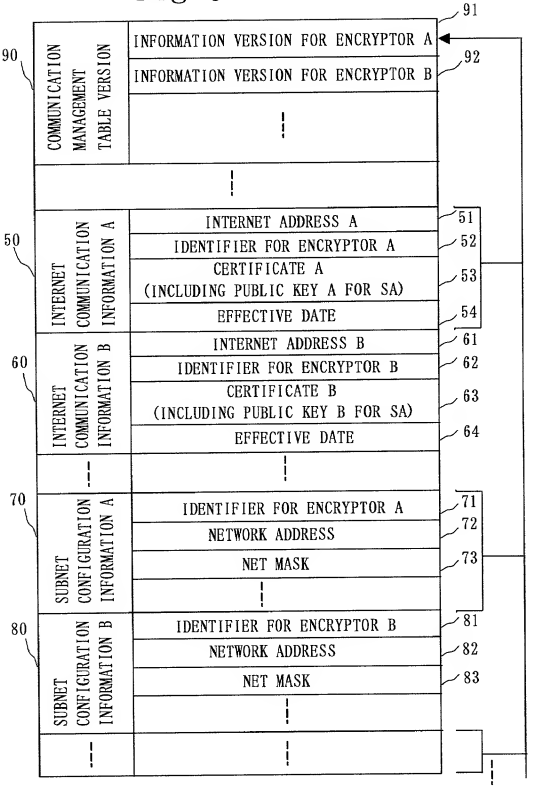
008068/60

Fig. 7



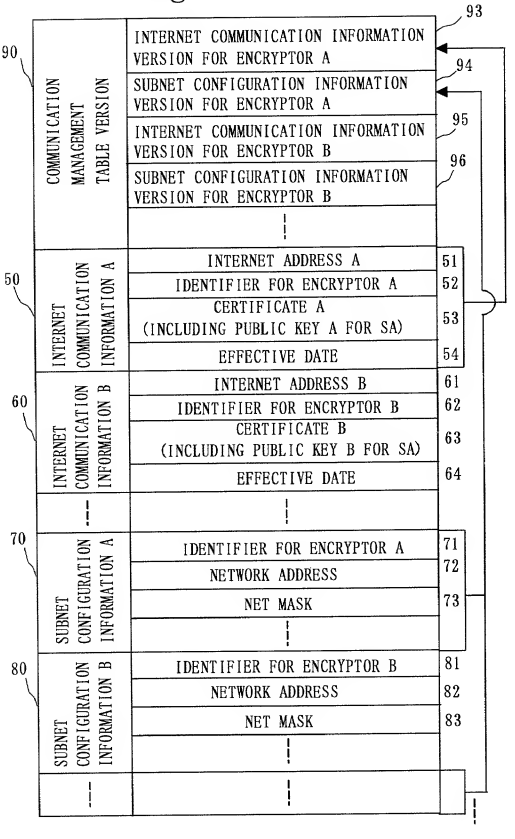
TOE080 "090600

Fig. 8



FOR 0880 "00806860

Fig. 9



TAE080-00806860

Fig. 10

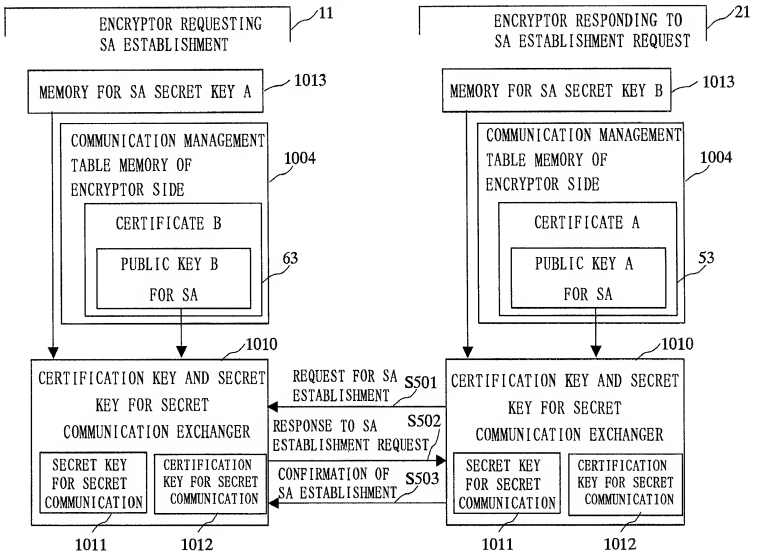
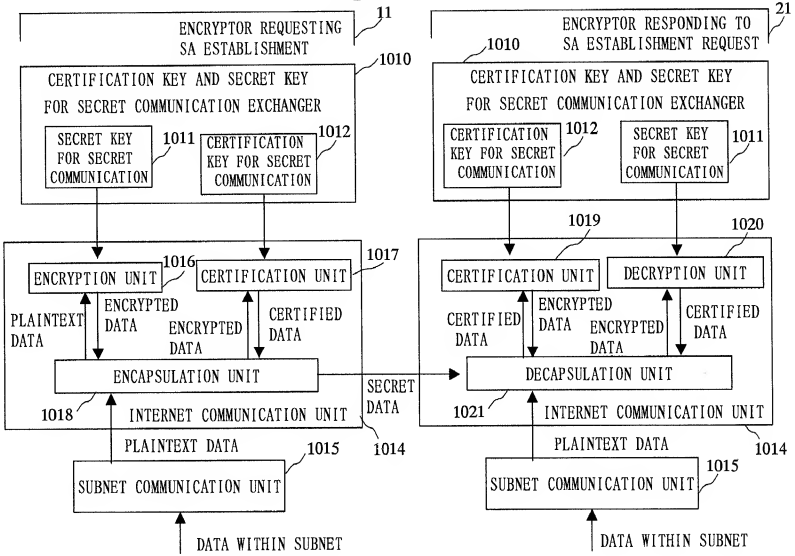

ENCRYPTOR REQUESTING SA ESTABLISHMENT
11
ENCRYPTOR RESPONDING TO SA ESTABLISHMENT REQUEST
21
MEMORY FOR SA SECRET KEY A
1013
MEMORY FOR SA SECRET KEY B
1013
COMMUNICATION MANAGEMENT TABLE MEMORY OF ENCRYPTOR SIDE
1004
CERTIFICATE B
PUBLIC KEY B FOR SA
63
COMMUNICATION MANAGEMENT TABLE MEMORY OF ENCRYPTOR SIDE
1004
CERTIFICATE A
PUBLIC KEY A FOR SA
53
1010
CERTIFICATION KEY AND SECRET KEY FOR SECRET COMMUNICATION EXCHANGER
SECRET KEY FOR SECRET COMMUNICATION
CERTIFICATION KEY FOR SECRET COMMUNICATION
1011
1012
REQUEST FOR SA ESTABLISHMENT
S501
RESPONSE TO SA ESTABLISHMENT REQUEST
S502
CONFIRMATION OF SA ESTABLISHMENT
S503
1010
CERTIFICATION KEY AND SECRET KEY FOR SECRET COMMUNICATION EXCHANGER
SECRET KEY FOR SECRET COMMUNICATION
CERTIFICATION KEY FOR SECRET COMMUNICATION
1011
1012

Fig. 11



09/830,660

Fig.12

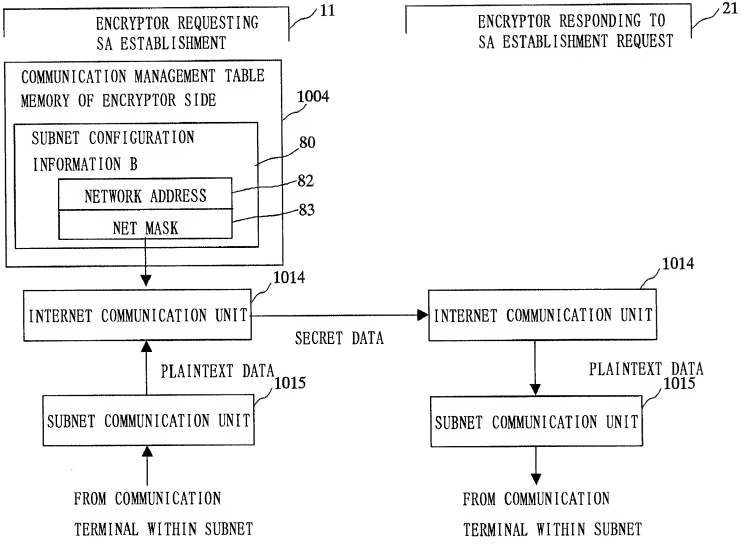
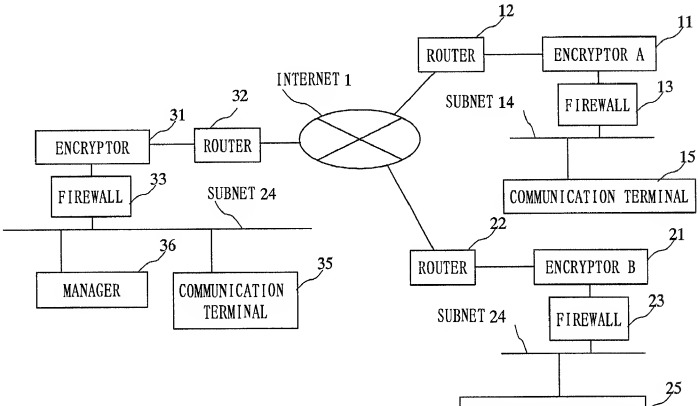

ENCRYPTOR REQUESTING SA ESTABLISHMENT
11
ENCRYPTOR RESPONDING TO SA ESTABLISHMENT REQUEST
21
COMMUNICATION MANAGEMENT TABLE MEMORY OF ENCRYPTOR SIDE
1004
SUBNET CONFIGURATION INFORMATION B
80
NETWORK ADDRESS
82
NET MASK
83
1014
INTERNET COMMUNICATION UNIT
SECRET DATA
INTERNET COMMUNICATION UNIT
1014
PLAINTEXT DATA
1015
SUBNET COMMUNICATION UNIT
PLAINTEXT DATA
1015
SUBNET COMMUNICATION UNIT
FROM COMMUNICATION TERMINAL WITHIN SUBNET
FROM COMMUNICATION TERMINAL WITHIN SUBNET

Fig. 13



09/830060

Fig. 14

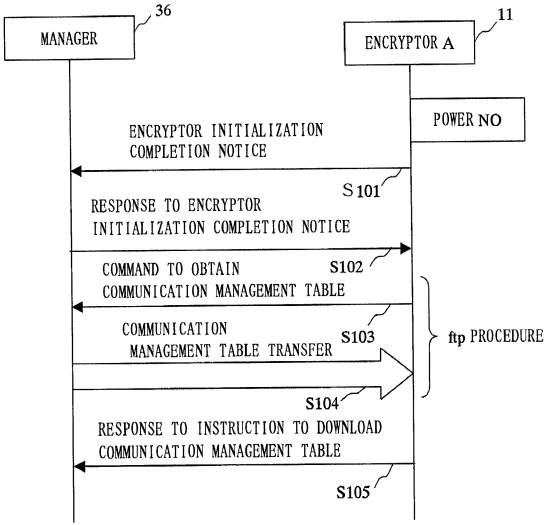
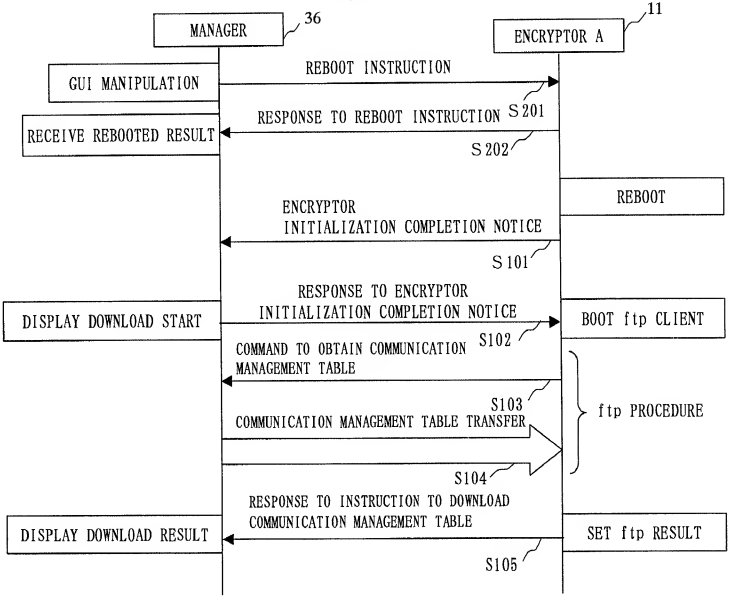

MANAGER
36
ENCRYPTOR A
11
POWER NO
ENCRYPTOR INITIALIZATION COMPLETION NOTICE
S101
RESPONSE TO ENCRYPTOR INITIALIZATION COMPLETION NOTICE
COMMAND TO OBTAIN COMMUNICATION MANAGEMENT TABLE
S102
COMMUNICATION MANAGEMENT TABLE TRANSFER
S103
ftp PROCEDURE
S104
RESPONSE TO INSTRUCTION TO DOWNLOAD COMMUNICATION MANAGEMENT TABLE
S105

Fig. 15


MANAGER
36
ENCRYPTOR A
11
GUI MANIPULATION
REBOOT INSTRUCTION
RESPONSE TO REBOOT INSTRUCTION
S201
RECEIVE REBOOTED RESULT
S202
REBOOT
ENCRYPTOR
INITIALIZATION COMPLETION NOTICE
S101
RESPONSE TO ENCRYPTOR
INITIALIZATION COMPLETION NOTICE
DISPLAY DOWNLOAD START
BOOT ftp CLIENT
S102
COMMAND TO OBTAIN COMMUNICATION
MANAGEMENT TABLE
S103
COMMUNICATION MANAGEMENT TABLE TRANSFER
ftp PROCEDURE
S104
RESPONSE TO INSTRUCTION TO DOWNLOAD
COMMUNICATION MANAGEMENT TABLE
DISPLAY DOWNLOAD RESULT
SET ftp RESULT
S105

JC05 Rec'd PCT/PTO 0 3 AUG 2001

U.S. APPLICATION NO. (If known, / see 37 C.F.R. 1.5(c))	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
Unassigned 09/890800	PCT/JP00/00474	018773-030

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1,000.00 (960)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $860.00 (970)		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $710.00 (958)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $690.00 (956)		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00 (962)		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 860.00	
Surcharge of **$130.00 (154)** for furnishing the oath or declaration later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	12 -20 =	0	X$18.00 (966)	$ 0	
Independent Claims	4 -3 =	1	X$80.00 (964)	$ 80.00	
Multiple dependent claim(s) (if applicable)			+ $270.00 (968)	$	
TOTAL OF ABOVE CALCULATIONS =				$ 940.00	
Reduction for 1/2 for filing by small entity, if applicable (see below).				$	-
SUBTOTAL =				$ 940.00	
Processing fee of $130.00 **(156)** for furnishing the English translation later than 20 ☐ 30 ☐ months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
TOTAL NATIONAL FEE =				$ 940.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 (581)** per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$ 980.00	
				Amount to be: refunded	$
				charged	$

a. ☐ Small entity status is hereby claimed.

b. ☒ A check in the amount of $ 980.00 to cover the above fees is enclosed.

c. ☐ Please charge my Deposit Account No. 02-4800 in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

d. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 02-4800. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Platon N. Mandros
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

William C Rowland RN 30888, for
SIGNATURE

Platon N. Mandros
NAME

22,124
REGISTRATION NUMBER

(01/01)

Declaration and Power of Attorney for Patent Application

特許出願宣告書及び委任状

Japanese Language Declaration

日本語宣告書

下記の氏名の発明者として、私は以下の通り宣言します。

As a below named inventor, I hereby declare that:

私の住所、私書箱、国籍は下記の私の氏名の後に記載された通りです。

My residence, post office address and citizenship are as stated next to my name.

下記の名称の発明に関して請求範囲に記載され、特許出願している発明内容について、私が最初かつ唯一の発明者（下記の氏名が一つの場合）もしくは最初かつ共同発明者であると（下記の名称が複数の場合）信じています。

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) or the subject matter which is claimed and for which a patent is sought on the invention entitled

_____

_____

_____

Communication Management Table Transfer System, Manager, Encryptor, and Communication Management Table Transfer Method

上記発明の明細書（下記の欄でx印がついていない場合は本書に添付）は、

the specification of which is attached hereto unless the following box is checked:

☐ _月_日に提出され、米国出願番号または特許協定条約国際出願番号を_____とし、（該当する場合）_____に訂正されました。

☑ was filed on January 28, 2000 as United States Application Number or PCT International Application Number PCT/JP00/00474 and was amended on _____ (if applicable).

私は、特許請求範囲を含む上記訂正後の明細書を検討し、内容を理解していることをここに表明します。

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

私は、連邦規則法典第３７編第１条５６項に定義されるとおり、特許資格の有無について重要な情報を開示する義務があることを認めます。

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

Japanese Language Declaration
（日本語宣告書）

私は、米国法典第３５編１１９条(a)-(d)項又は３６５条(b)項に基づき下記の、米国以外の国の少なくとも一ヶ国を指定している特許協力条約３６５(a)項に基づく国際出願、又は外国での特許出願もしくは発明者証の出願についての外国優先権をここに主張するとともに、優先権を主張している、本出願の前に出願された特許または発明者証の外国出願を以下に、枠内をマークすることで、示しています。

I hereby claim foreign priority under Title 35, United States Code, Section 119 (a)-(d) or 365(b) of any foreign application(s) for patent or Inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or Inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)
外国での先行出願

Priority Not Claimed
優先権主張なし

Number (番号)	Country (国名)	Day/Month/Year Filed (出願の年月日)	☐
Number (番号)	Country (国名)	Day/Month/Year Filed (出願の年月日)	☐

私は、第３５編米国法典１１９条(e)項に基づいて下記の米国特許出願規定に記載された権利をここに主張いたします。

I hereby claim the benefit under Title 35, United States Code, Section 119 (e) of any United States provisional application(s) listed below

Application No. (出願番号)	Filing Date (出願日)	Application No. (出願番号)	Filing Date (出願日)

私は、下記の米国法典第３５編１２０条に基づいて下記の米国特許出願に記載された権利、又は米国を指定している特許協力条約３６５条(c)に基づく権利をここに主張します。また、本出願の各請求範囲の内容が米国法典第３５編１１２条第１項又は特許協力条約で規定された方法で先行する米国特許出願に開示されていない限り、その先行米国出願書提出日以降で(c)本出願書の日本国内または特許協力条約国際提出日までの期間中に入手された、連邦規則法典第３７編１条５６項で定義された特許資格の有無に関する重要な情報について開示義務があることを認識しています。

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s), or 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of application.

Application No. (出願番号)	Filing Date (出願日)	Status : Patented, Pending, Abandoned (現況：特許許可済、係属中、放棄済)

私は、私自身の知識に基づいて本宣告書中で私が行う表明が真実であり、かつ私の入手した情報と私の信じるところに基づく表明が全て真実であると信じていること、さらに故意になされた虚偽の表明及びそれと同等の行為は米国法典第１８編第１００１条に基づき、罰金または拘禁、もしくはその両方により処罰されること、そしてそのような故意による虚偽の声明を行えば、出願した、又は既に許可された特許の有効性が失われることを認識し、よってここに上記のごとく宣誓を致します。

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Japanese Language Declaration
(日本語宣告書)

委任状： 私は下記の発明者として、本出願に関する一切の手続きを米特許商標局に対して遂行する弁理士または代理人として、下記の者を指名いたします。(弁理士、または代理人の氏名及び登録番号を明記のこと)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (*list name and registration number*)

William L. Mathis	17,337	Ralph L. Freeland, Jr.	16,110	William C. Rowland	30,888
Peter H. Smolka	15,913	Robert G. Mukai	28,531	T.Gene Dillahunty	25,423
Robert S. Swecker	19,885	George A. Hovanec, Jr.	28,223	Anthony W. Shaw	30,104
Platon N. Mandros	22,124	James A. LaBarre	28,632	Patrick C. Keane	32,858
Benton S. Duffett, Jr.	22,030	E. Joseph Gess	28,510	Bruce J. Boggs, Jr.	32,344
Joseph R. Magnone	24,239	R. Danny Huntington	27,903	William H. Benz	25,952
Norman H. Stepno	22,716	Eric H. Weisblatt	30,505	Peter K. Skiff	31,917
Ronald L. Grudziecki	24,970	James W. Peterson	26,057	Richard J. McGrath	29,195
Frederick G. Michaud, Jr.	26,003	Teresa Stanek Rea	30,427	Matthew L. Schneider	32,814
Alan E. Kopecki	25,813	Robert E. Krebs	25,885	Michael G. Savage	32,596
Regis E. Slutter	26,999	Robert M. Schulman	31,196	Gerald F. Swiss	30,113
Samuel C. Miller	27,360				

34

直接電話連絡先： (名前及び電話番号)

Direct Telephone Calls to. (*name and telephone number*)

Platon N. Mandros
703/836-6620

唯一のまたは第一発明者名		Full Name of sole or first Inventor Noriko Takeda
発明者の署名	日付	First inventor's signature Date Noriko Takeda May 18,2001
住所		Residence Tokyo, Japan
国籍		Citizenship Japan
私書箱		Post Office Address c/o Mitsubishi Electric Systemware Corporation 12-1, Yurakucho 1-chome, Chiyoda-ku, Tokyo 100-0006, Japan
第二共同発明者の氏名		Full Name of second joint inventor, if any Akihiko Sasamoto
第二発明者の署名	日付	Second inventor's signature Date Akihiko Sasamoto May 18,2001
住所		Residence Tokyo, Japan
国籍		Citizenship Japan
私書箱		Post Office Address c/o Mitsubishi Denki Kabushiki Kaisha 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, Japan

(第三以降の共同発明者についても同様に記載し、署名をすること)

(Supply similar information and signature for third and subsequent joint inventors.)

Japanese Language Declaration

第三共同発明者の氏名 3-00	Full Name of third joint inventor, if any Kazuyuki Adachi
第三発明者の署名 日付	Third inventor's signature Date Kazuyuki Adachi May. 25. 2001
住所	Residence Tokyo, Japan JPX
国籍	Citizenship Japan
私書箱	Post Office Address c/o Mitsubishi Denki Kabushiki Kaisha 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, Japan

第四共同発明者の氏名 4-00	Full Name of fourth joint inventor, if any Seiichi Shinoda
第四発明者の署名 日付	Fourth inventor's signature Date Seiichi Shinoda May. 18 2001
住所	Residence Tokyo, Japan JPX
国籍	Citizenship Japan
私書箱	Post Office Address c/o Mitsubishi Denki Kabushiki Kaisha 2-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo 100-8310, Japan

第五共同発明者の氏名	Full Name of fifth joint inventor, if any
第五発明者の署名 日付	Fifth inventor's signature Date
住所	Residence
国籍	Citizenship
私書箱	Post Office Address

第六共同発明者の氏名	Full Name of sixth joint inventor, if any
第六発明者の署名 日付	Sixth inventor's signature Date
住所	Residence
国籍	Citizenship
私書箱	Post Office Address

(第七またはそれ以降の共同発明者に対しても同様な情報及び署名を提供すること。) (Supply similar information and signature for seventh and subsequent joint inventors.)